Impact of Critical Node Failures on Lifetime of UWSNs with Incomplete Secure Connectivity

Burak Emre Un*†, Huseyin Ugur Yildiz‡, and Bulent Tavli§

*TOBB University of Economics and Technology, 06560, Ankara, Turkey, e-mail: burakemreun@etu.edu.tr
†Radar and EW Systems Vice Presidency, ASELSAN Inc., 06830, Ankara, Turkey, e-mail: beun@aselsan.com.tr
‡TED University, 06420, Ankara, Turkey, e-mail: hugur.yildiz@tedu.edu.tr
§TOBB University of Economics and Technology, 06560, Ankara, Turkey, e-mail: btavli@etu.edu.tr

***Abstract*—Underwater wireless sensor networks (UWSNs) are, typically, comprised of sparsely deployed sensor nodes in hostile areas. Security of data flows among nodes are established by encryption of data packets, however, due to the limited memory of the sensor nodes, only a subset of keys distributed to the whole network exists at each node, therefore, only a subset of available physical links can be used for secure communications. Indeed, two neighbor sensor nodes can establish secure connectivity only if they share a common key, therefore, the existence of a physical link between a node pair is not sufficient to establish direct secure communications if they do not share a common key. Incomplete secure connectivity makes UWSNs more vulnerable to critical node failures because of the reduction in alternative paths towards the base station. In fact, it is possible to reduce the network lifetime of UWSNs significantly by incapacitating the most critical node in a given deployment topology, which is exacerbated by incomplete secure connectivity. Such nodes, typically, are found in close proximity to the base station. In this study, a linear programming (LP) model is developed to explore the effects of critical node failures on the lifetime of UWSNs with incomplete secure connectivity. Our results reveal that critical node incapacitation can reduce the network lifetimes by up to 47% while increasing the energy consumption overhead of the network by up to 46%.**

***Index Terms*—underwater wireless sensor networks, node capture attack, secure connectivity, network lifetime, optimization.**

I. Introduction

Oceans covering more than 70% of the earth's surface contain a large amount of data about the underwater environment, which are still unexplored. Underwater wireless sensor networks (UWSNs) are deemed as a promising technology for Internet of Underwater Things and they can be considered as a feasible solution to explore the undiscovered aquatic habitat [1]. UWSNs are generally used for military, commercial, and scientific monitoring purposes [2]. A typical UWSN consists of numerous sensor nodes and a sink node. Sensor nodes have limitations on the battery energy, and they are randomly deployed for generating data about the underwater environment. The sink node, which is assumed to have no constraints on the battery power and located on the surface of the water, collects the data generated by the sensor nodes [3]. Recharging or replacing the batteries of sensor nodes is impractical once they are deployed. Thus, it is crucial to establish energy-efficiency among the sensor nodes to elongate the operational lifespan of the UWSNs [4].

In UWSNs, radio waves cannot be directly used for data communications since these waves rapidly attenuate in underwater environment. Instead, acoustic waves are considered a feasible alternative for underwater communications [5]. However, acoustic communications have several handicaps, including low bandwidth, high error rates, and long propagation delay [6]. Moreover, UWSN nodes are sparsely deployed in inaccessible and hostile areas. Due to the challenges of underwater communications and the sparse deployment of sensor nodes, UWSNs are vulnerable to various security threats [7].

The underwater environment is an excellent theatre for performing eavesdropping attacks to extract secret information from the traffic flowing among the nodes of UWSNs [8]. As a countermeasure for this potential security threat, which is extremely challenging to detect due to the passive listening of a potential eavesdropper, is to encrypt data flows among the nodes through the use of pre-distributed encryption keys [9]. Typically, cryptographic keys are distributed to each node randomly before the actual deployment. Each node possesses a subset of the whole key pool because of the limited memory space of sensor nodes and also as a precaution against node capture attacks [10]. If each node is loaded with the whole key pool then in the case of the capture of any of the nodes in the UWSN security of the whole network will be compromised. As an alternative, pairwise shared keys can be used, such that a secure link is generated between two nodes as long as they share a common key. In this case, if a node is captured, only the communication between the relevant node pairs will be compromised rather than the entire network [11].

Since each node has only a subset of the entire key pool, some neighboring node pairs (even if they can establish a direct communication link between them) cannot establish secure connectivity if they do not share a common key. This is known as *incomplete secure connectivity*, which reduces the number of usable secure links in the network. In many UWSN applications, a *converge-cast* (many-to-one) traffic pattern is adopted, and energy imbalance among the nodes remains a major problem as *hot spots* are created around the sink node. Nodes in the hot spots need to convey a large amount

of network traffic hence they dissipate their battery energies rapidly. If the network lifetime is defined as the time until the first node dies, then the hot spot problem can result in short network lifetimes [12]. Even worse, it is possible to completely incapacitate the network by compromising one or more critical nodes in the hot spot. Nevertheless, by reducing the number of alternative routes comprised of secure links (when compared to the number of links without any security constraint), the burden and criticality of certain nodes increases. Incapacitation of such nodes can potentially impact network lifetime significantly.

The existing literature on security in UWSNs is rich, and new research results are being added to the literature day-to-day. Security issues in UWSNs, common threat types and countermeasures against the malicious attacks are surveyed in [5], [6], [8], [13]. Most research on node capture attacks has been carried out for terrestrial WSNs instead of UWSNs. Some important studies on the node capture attacks in terrestrial WSNs are summarized as follows. In [14], several security schemes for node capture attacks are discussed. In [15], the concept of the one-time sensor for mitigating node capture attacks is proposed, where each node is loaded with only one cryptographic token before deployment. In [16], an integer programming model is presented for modeling node capture attacks in heterogeneous WSNs. In [17], the authors develop a computationally efficient secure localization algorithm to mitigate node capture attacks. In [18], an efficient and low energy cost node matrix-based capture attack method is developed, where a matrix is used to determine the compromise between the nodes and paths. In [19], a protocol is proposed that uses hash-based keys and pseudo-random functions for detecting the node capture attacks.

There is a growing body of literature that is concerned with key distribution schemes for both terrestrial WSNs and UWSNs. In [20], a probabilistic key distribution method is proposed where each sensor node randomly picks a set of keys from a key pool before the deployment. In [9], a key distribution scheme for peer-to-peer communication is developed for mobile UWSNs. In [21], a security framework called SecFUN (*i.e.*, Security Framework for Underwater acoustic sensor Networks) for UWSNs is introduced, where each sensor node shares the same group key and a unique secret key with the sink node. Luo *et al.* [22] discuss received-signal-strength-based key generation approaches in UWSNs. In [23], a hexagon-based key distribution mechanism for acoustic sensor networks is proposed. In [24], chaotic maps remote user authentication and a key agreement scheme are developed for UWSNs, which can boycott the node capture attacks. In [25], quantum and symmetric cryptography are jointly used to improve communication security in UWSNs.

In our earlier works, [26] and [27], we separately analyzed the effects of failure of critical nodes and incomplete secure connectivity problems on the lifetime of terrestrial WSNs, respectively. However, the joint impact of critical node failures and incomplete secure connectivity issues on the network lifetime remains unclear in UWSNs literature. In this paper, we consider UWSNs with incomplete secure connectivity, where some links are secured by adopting the probabilistic key pre-distribution scheme as in [20]. We develop a linear programming (LP) model that finds optimal secured routes from the source nodes to the sink node to maximize the UWSNs lifetime. Furthermore, the LP framework is used to identify the critical nodes that would reduce the network lifetime most.

II. System Model

A. Network Architecture

The network architecture is composed of $|\mathcal{W}|$ static sensor nodes and a single sink node (node-1), where we define $\mathcal{W}$ to be the set of all sensor nodes in the UWSN. Thus, we describe the network topology with the directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{A})$, where $\mathcal{V} = \mathcal{W} \cup \{1\}$ and $\mathcal{A}$ are the sets of all nodes (including the sink node) and all links in the UWSN.

Sensor nodes are assumed to be homogeneous in terms of battery capacity, where the initial battery of each sensor node is defined as ε_{bat}. Moreover, sensor nodes have a maximum transmission range d_{max}, and nodes can adjust their transmission power in a continuous manner depending on the distance between the source and the destination node. Sensor nodes are uniformly distributed in a three-dimensional rectangular volume, $d_e \times d_e \times h$ m^3, where d_e is the edge length (in m) and h is the depth of water (in m). Sensor node locations are assumed to be static in the water. The sink node is positioned on the surface of the water and located at one of the corners of the network. Following the fundamental principles detailed in [20], [27], we assume that each link is secured with probability P_{ksp} (*i.e.*, at least one cryptographic key is shared between two nodes). Data generated by the sensor nodes reach the sink node

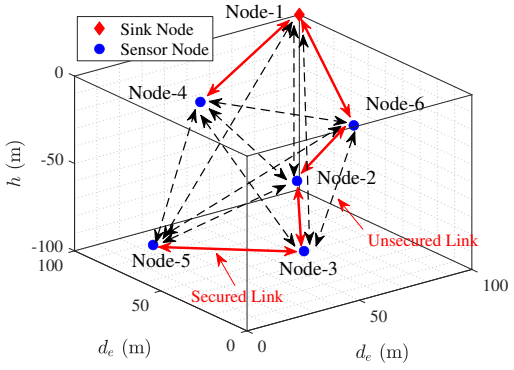


Fig. 1: An example network architecture with $|\mathcal{W}| = 5$ sensor nodes and a sink node, where $d_e = h = 100$ m.

either by direct transfer or through other sensors relaying data to the sink node. We adopt the network lifetime definition given in [12], which is the time elapsed when the first sensor node consumes all of its battery power.

In Fig. 1, we provide an example of our network architecture, which consists of $|\mathcal{W}| = 5$ sensor nodes and a sink node. In this network architecture, links (3,5), (3,2), (2,6), (4,1), and

(6,1) are secured (illustrated with red solid double arrow), while the other links are unsecured (pictured with black dashed double arrow). For example, node-5 needs to use the multi-hop path 5-3-2-6-1 to convey its data to the sink node securely. On the other hand, node-4 can directly transmit its data to the sink node (single hop).

B. Underwater Energy Consumption Model

We utilize the energy dissipation model detailed in [28], [29], for calculating the transmission and reception energy costs of one bit in the underwater environment. The acoustic path loss between node-i and node-j is expressed as

$$A(d_{ij}, f) = (d_{ij})^k \times \alpha(f)^{10^{-3} \times d_{ij}}, \tag{1}$$

where k is the spreading factor, f is the operating frequency (in kHz), d_{ij} is the distance between node-i and node-j (in m), and $\alpha(f)$ is the absorption coefficient. The absorption coefficient is calculated (in dB/km) with Thorp's formula as

$$10\log_{10}\alpha(f) = \frac{0.11 f^2}{1+f^2} + \frac{44 f^2}{4100+f^2} + 2.75 \cdot 10^{-4} f^2 + 0.003. \tag{2}$$

The energy required to transmit one bit of data from node-i to node-j is defined as

$$E_{tx}(d_{ij}) = A(d_{ij}, f) \times P_0, \tag{3}$$

where P_0 is the desired power level at the input to the receiver. The reception energy cost per bit is constant and presented as

$$E_{rx} = P_r, \tag{4}$$

where P_r depends on the underwater node platform.

C. LP Model to Maximize UWSNs Lifetime with Incomplete Secure Connectivity

We introduce our LP model, which maximizes UWSNs lifetime with incomplete secure connectivity, in (5).

$$\text{Max. } t \tag{5a}$$

subject to:

$$\sum_{j \in \mathcal{V}} g_{ij} - \sum_{j \in \mathcal{W}} g_{ji} = \begin{cases} s_i \times t, & \forall i \in \mathcal{W} \\ -\sum_{j \in W} s_j \times t, & i = 1 \end{cases} \tag{5b}$$

$$g_{ij} \geq 0,\ i \neq j,\ \forall (i,j) \in \mathcal{A} \tag{5c}$$

$$\sum_{j \in \mathcal{V}} g_{1j} = 0 \tag{5d}$$

$$g_{ij} = 0 \text{ if } d_{ij} > d_{\max},\ \forall (i,j) \in \mathcal{A} \tag{5e}$$

$$\sum_{j \in \mathcal{V}} E_{tx}(d_{ij}) \times g_{ij} + E_{rx} \sum_{j \in \mathcal{W}} g_{ji} = \varepsilon_i,\ \forall i \in \mathcal{W} \tag{5f}$$

$$\varepsilon_i \leq \varepsilon_{\text{bat}},\ \forall i \in \mathcal{W} \tag{5g}$$

$$g_{ij} = \begin{cases} g_{ij} & \text{if } \beta_{ij} \leq P_{\text{ksp}} \\ 0 & \text{o.w.} \end{cases},\ \forall (i,j) \in \mathcal{A}. \tag{5h}$$

The objective function of the LP model is the maximization of the network lifetime (*i.e.*, the time elapsed until the first node drains its battery energy). We use the free decision variable, t, in (5a) for representing the network lifetime in terms of seconds. In the LP model we define two continuous decision variables, where g_{ij} and ε_i are the number of bits flowing from node-i to node-j and the energy consumed by node-i through the network lifetime, respectively. The constraints of the LP model are given in (5b)–(5h). Const. (5b) provides the flow conservation at each sensor node-i ($\forall i \in \mathcal{W}$) and the sink node ($i = 1$). In this constraint, the parameter s_i shows the data generation rate at each sensor node (in terms of bits per second). Const. (5c) ensures that the network traffic is always non-negative. Furthermore, this constraint eliminates possible loops at each source node-i, such that the generated flows cannot be terminated at source nodes. Const. (5d) forces the sink node to collect data from source nodes rather than generating data. Const. (5e) imposes the maximum communication range constraint for each transmitting node. Const. (5f) calculates the total energy dissipated for transmission (*i.e.*, $\sum_{j \in \mathcal{V}} E_{tx}(d_{ij}) \times g_{ij}$) and reception (*i.e.*, $E_{rx} \sum_{j \in \mathcal{W}} g_{ji}$) by each sensor node-$i$ through the network lifetime (*i.e.*, ε_i). Note that $E_{tx}(d_{ij})$ and E_{rx} are the transmission and reception energy costs per bit, which have been already derived in Eqs. (3) and (4), respectively. Const. (5g) limits the total energy consumption of a sensor node to the initial battery energy (ε_{bat}). Finally, Const. (5h) allows data to be flowed over a secured link. In this constraint, β_{ij} is assumed to be a uniform random variable in (0,1). If node-i and node-j share a common key (when $\beta_{ij} \leq P_{\text{ksp}}$), the data flow is allowed over this secured acoustic channel. We assume that links are symmetric hence, $\beta_{ij} = \beta_{ji}$. In summary, the LP framework finds the best secure routes between each source node and the sink node to maximize the network lifetime. In fact, flows within the network are optimized to avoid the premature energy depletion of any sensor node.

D. Node Incapacitation Model

We assume that the cause of node incapacitation is node capture attacks. However, we assume that captured nodes are physically destroyed and their keys are not compromised. The node capture attack model is presented in Algorithm 1. Our attack model identifies the sensor nodes that should be removed from the network topology for yielding the shortest lifetimes. We start by randomly generating a network topology and define N_C to show the number of nodes to be compromised. Then, a single sensor node from the network is removed sequentially (lines 2–4). The excluded node is represented as v_i, where it can be considered as the first *potential* captured node. The LP model in (5) is solved when v_i is removed from the network, and the corresponding network lifetime is recorded as t_i (line 5). Note that t_i is the network lifetime obtained when node-i is seized. In each step, we only remove one sensor node and calculate t_i value (line 6). After all t_i values are obtained, we find the value of i for which t_i is the minimum (line 8). The lowest lifetime value is included in the set, $\mathcal{T}_k$, which is the final lifetime when the first critical node is compromised (line 9). Furthermore,

Algorithm 1 Node Capture Attack Model

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{A})$: the network topology, N_C: the number of captured critical nodes.

Output: $\mathcal{C}$: set of the most critical captured nodes, $\mathcal{T}$: set of the network lifetimes when nodes in $\mathcal{C}$ are captured.

1: Define $\mathcal{C} = \{\mathcal{C}_k\}_{k=1}^{N_C} = \emptyset$ and $\mathcal{T} = \{\mathcal{T}_k\}_{k=1}^{N_C} = \emptyset$;
2: **for** $k = 1$ to N_C **do**
3: **for** $i = 2$ to $|\mathcal{V}|$ **do**
4: Remove node-i (*i.e.*, v_i) from the network;
5: Solve the LP model in (5) without v_i;
6: Record the network lifetime as t_i (*i.e.*, $t_i \leftarrow t$);
7: **end for**
8: Find the value of i for which t_i is the minimum;
9: Store the minimum t_i value in the set $\mathcal{T}_k$, $\mathcal{T}_k \leftarrow \min_i\{t_i\}$;
10: Store the most critical captured node-i in the set $\mathcal{C}_k$, $\mathcal{C}_k \leftarrow v_j,\ j = \text{argmin}_i\{t_i\}$;
11: Update the network topology by removing the most critical captured node, $\mathcal{G} \leftarrow \mathcal{G} \setminus \mathcal{C}_k$;
12: **end for**
13: **Result:** $\mathcal{C} = \bigcup_{k=1}^{N_C} \mathcal{C}_k$ and $\mathcal{T} = \bigcup_{k=1}^{N_C} \mathcal{T}_k$

the critical node, v_i, yielding the minimum t_i is included in the set of captured nodes, $\mathcal{C}_k$ (line 10). After finding the first critical node, this node is completely separated from the network, and the network topology is updated (line 11). The remaining $N_C - 1$ critical nodes are obtained by following the procedure as described above. Finally, the sets of the most critical captured nodes ($\mathcal{C}$) and the network lifetimes when a total of N_C nodes are compromised ($\mathcal{T}$) are returned (line 13).

III. Performance Evaluation

In this section, we provide the results of our numerical analysis for investigating the effects of node incapacitation occurrences on lifetime of UWSNs with incomplete secure connectivity. The LP model described in (5) and the node capture attack model stated in Algorithm 1 are developed in GAMS (https://www.gams.com/) and solved using the CPLEX solver. We randomly generate 50 network topologies, and each result displayed in Figs. 2–4 is averaged over fifty random network topologies. For solving the LP framework and the node capture attack model, we utilize the parameters given in Table I.

We provide the drop in UWSN lifetimes when the network is under node capture attacks as a function of key sharing probability (P_{ksp}) for three network edge sizes, $d_e = 500$ m, 1000 m, and 1500 m in Figs. 2a, 2b, and 2c, respectively. In other words, in this figure, we reveal how much the network lifetime (obtained in the absence of node capture attacks) decreases when critical nodes are compromised. In each subplot, we display three curves that show the number

TABLE I: Analysis parameters.

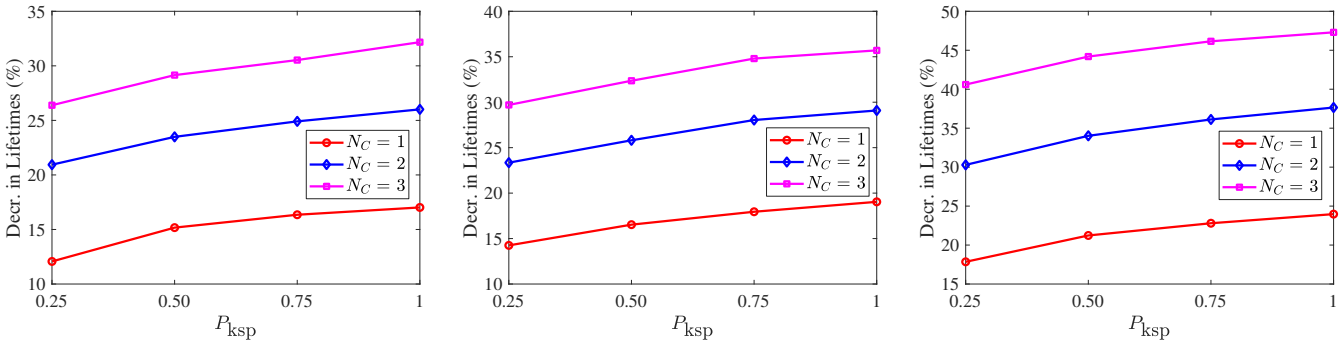
Param.	Description	Value
d_{max}	Max. commun. range (m)	1000 [30]
d_e	Edge size of the network (m)	{500, 1000, 1500}
ε_{bat}	Battery energy (KJ)	10
f	Operating frequency (kHz)	10
h	Depth of the network (m)	500
k	Spreading factor	1.5 [30]
N_C	Number of captured nodes	{0, 1, 2 ,3} [26]
P_{ksp}	Key sharing probability	{0.25, 0.5, 0.75, 1} [27]
$\|\mathcal{W}\|$	Number of sensor nodes	50 [26]
P_0	Desired power at the input to the receiver (J/bit)	1×10^{-7} [30]
P_r	Reception constant (J/bit)	0.2×10^{-7} [30]
s_i	Data generation rate (bps)	1 [27]

of nodes that are captured (N_C) and we calculate the percent decrement in network lifetimes for the three N_C values when P_{ksp} is constant. The drop in network lifetimes is the lowest when $P_{\text{ksp}} = 0.25$ and the highest when $P_{\text{ksp}} = 1$. Our results show that node capture attacks reduce the network lifetimes by 12% at least (when $N_C = 1$ and $P_{\text{ksp}} = 0.25$ in Fig. 2a) and 47% at most (when $N_C = 3$ and $P_{\text{ksp}} = 1$ in Fig. 2c). The percent decrement in network lifetimes raises as P_{ksp} increases for a fixed N_C. For example, in Fig. 2c when $N_C = 3$, percent decrement in network lifetimes grows from 41% to 47% as P_{ksp} is raised from 0.25 to 1. The reason behind this trend is that when the connectivity of the network increases as P_{ksp} grows, the number of nodes that are included in the hot spot of the network also increases. Hence, capturing one or more nodes in the hot spot would have a devastating impact on the network lifetime. Similarly, as N_C rises for a constant P_{ksp}, the percent decrement in network lifetimes grows since eliminating more critical nodes imposes a considerably high energy burden on the remaining nodes. For instance, in Fig. 2a when $P_{\text{ksp}} = 0.25$, the drop in network lifetimes increases from 12% to 26% as N_C is elevated from 1 to 3. Finally, the sparseness of the network significantly rises the percent decrement in network lifetimes.

Figs. 3a, 3b, and 3c show the percent increments in the average energy consumption overhead, when the network is under node capture attacks, with respect to P_{ksp} for $d_e = 500$ m, 1000 m, and 1500 m, respectively. The average energy consumption overhead (*i.e.*, $\widetilde{\varepsilon}$) is defined as the average energy consumed per node per unit time, which is calculated as

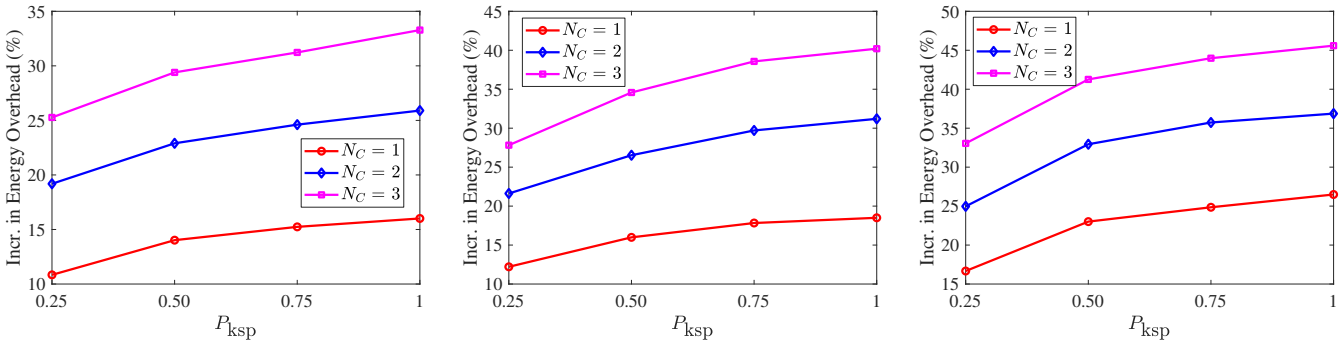
$$\widetilde{\varepsilon} = \frac{\sum_{i \in \mathcal{W}} \varepsilon_i}{t \times |\mathcal{W}|}. \tag{6}$$

For each P_{ksp} value, the percent rise in $\widetilde{\varepsilon}$ for the three N_C values are calculated according to the $\widetilde{\varepsilon}$ values obtained in the absence of node capture attacks. The results show that the minimum and the maximum percent increments in average energy consumption overhead are obtained as 11% (in Fig. 3a for $N_C = 1$ and $P_{\text{ksp}} = 0.25$) and 46% (in Fig. 3c for $N_C = 3$ and $P_{\text{ksp}} = 1$), respectively. The average energy consumption overhead increases as P_{ksp} grows when N_C is kept constant.



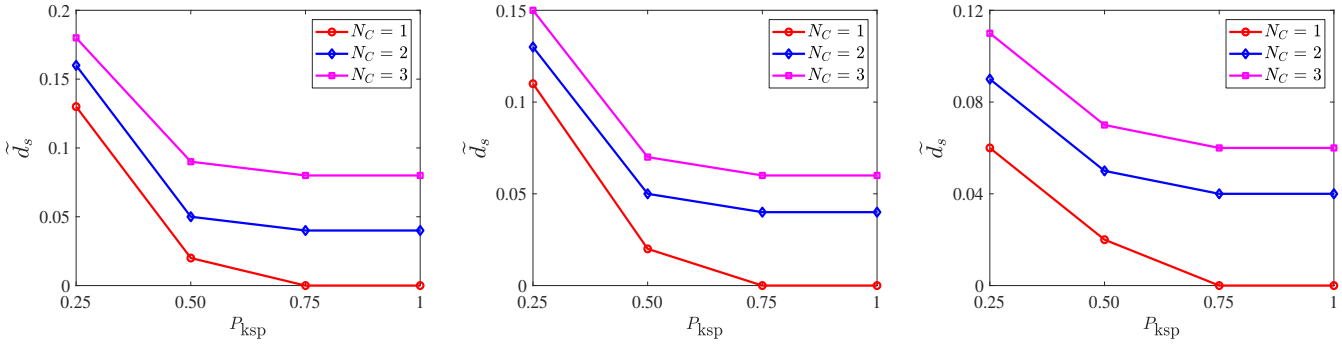
(a) $d_e = 500$ m (b) $d_e = 1000$ m (c) $d_e = 1500$ m

Fig. 2: Decrement in network lifetimes (%) as a function of P_{ksp} for three N_C and d_e values.



(a) $d_e = 500$ m (b) $d_e = 1000$ m (c) $d_e = 1500$ m

Fig. 3: Increment in energy consumption overhead (%) as a function of P_{ksp} for three N_C and d_e values.



(a) $d_e = 500$ m (b) $d_e = 1000$ m (c) $d_e = 1500$ m

Fig. 4: Avg. normalized distance of the captured nodes to the sink node ($\widetilde{d}_s$) wrt. P_{ksp} for three N_C and d_e values.

For example, when $N_C = 3$ and $d_e = 1500$ m, the percent increments in $\widetilde{\varepsilon}$ are calculated as 33%, 41%, 44%, and 46% for $P_{\text{ksp}} = 0.25$, 0.50, 0.75, and 1, respectively. Similarly, as N_C rises for a fixed P_{ksp} value, the percent increment in $\widetilde{\varepsilon}$ also grows. For instance, as N_C is elevated from 1 to 3 when $d_e = 500$ m and $P_{\text{ksp}} = 0.25$, the increment in $\widetilde{\varepsilon}$ changes from 11% to 25%.

We present the average normalized distances of the captured nodes to the sink node for the chosen P_{ksp} values when $d_e = 500$ m, 1000 m, and 1500 m in Figs. 4a, 4b, and 4c, respectively. The average normalized distance is denoted by $\widetilde{d}_s$ and calculated according to the following formula

$$\widetilde{d}_s = \frac{1}{N_C} \sum_{k \in \mathcal{C}} \frac{d_{k1} - \min_{i \in \mathcal{W}}\{d_{i1}\}}{\max_{i \in \mathcal{W}}\{d_{i1}\} - \min_{i \in \mathcal{W}}\{d_{i1}\}}. \tag{7}$$

In this formula, $\min_{i \in \mathcal{W}}\{d_{i1}\}$ and $\max_{i \in \mathcal{W}}\{d_{i1}\}$ are the distances between the sink node and the sensor node closest and farthest to the sink node, respectively. d_{k1} is the distance between the sink node and the captured node-k. By averaging over all captured nodes, given in set $\mathcal{C}$, we calculate the normalized distances. In summary, when $\widetilde{d}_s = 0$, the node

closest to the sink node is captured. On the other hand, when $\widetilde{d}_s = 1$, the farthest node to the sink node is compromised.

In each subfigure of Fig. 4, three N_C curves are presented as d_e is fixed. Our results reveal that normalized distances are observed as 0.18, 0.15, and 0.11 at most for $d_e = 500$ m, 1000 m, and 1500 m, respectively, when $P_{\text{ksp}} = 0.25$. As P_{ksp} increases, normalized distances reduce since nodes closest to the sink node have high chances of becoming critical nodes for node capture attacks. Moreover, $P_{\text{ksp}} \geq 0.75$ has an insignificant impact on $\widetilde{d}_s$ values of the compromised nodes. Regardless of the network sparseness, $\widetilde{d}_s = 0$ for $P_{\text{ksp}} \geq 0.75$ and $N_C = 1$, which means that nodes closest to the sink node are always captured. Normalized distances increase as N_C grows since more nodes close to the sink node are needed to be captured for yielding the shortest network lifetime. Note that increasing the sparsity of the network helps $\widetilde{d}_s$ values to be reduced.

IV. Conclusion

In this study, we investigate the impact of node incapacitation on the lifetime of UWSNs with incomplete secure connectivity. We utilized an LP model that determines secure routing paths from source nodes to the sink node to maximize the network lifetime, which is also the basis of our node capture attack algorithm for detecting the critical nodes reducing network lifetime the most. We solve the LP framework to optimality and operate the node capture attack model for various network configuration parameters such as network sparsity, key sharing probability, number of captured nodes, *etc.* The results show that node capture attacks can reduce the network lifetimes by 12% at least (for dense networks) and 47% at most (for sparse networks). Furthermore, node capture attacks raise the energy consumption overhead of the network between 11% and 46%. Nodes in 18% proximity to the sink node are typically the most vulnerable targets, which reduce the network lifetime most when incapacitated.

References

[1] E. Felemban, F. K. Shaikh, U. M. Qureshi, A. A. Sheikh, and S. B. Qaisar, "Underwater sensor network applications: A comprehensive survey," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 11, p. 896832, 2015.

[2] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad Hoc Netw.*, vol. 3, no. 3, pp. 257–279, 2005.

[3] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: An energy efficient routing protocol for UWSNs in the internet of underwater things," *IEEE Sens. J.*, vol. 16, no. 11, pp. 4072–4082, 2016.

[4] G. Han, S. Shen, H. Song, T. Yang, and W. Zhang, "A stratification-based data collection scheme in underwater acoustic sensor networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10 671–10 682, 2018.

[5] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, 2015.

[6] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wirel. Commun.*, vol. 18, no. 1, pp. 22–28, 2011.

[7] J. Jiang, G. Han, L. Shu, S. Chan, and K. Wang, "A trust model based on cloud theory in underwater acoustic sensor networks," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 342–350, 2017.

[8] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, "Challenges and security issues in underwater wireless sensor networks," *Procedia Comput. Sci.*, vol. 147, pp. 210–216, 2019.

[9] K. Kalkan and A. Levi, "Key distribution scheme for peer-to-peer communication in mobile underwater wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 4, pp. 698–709, 2014.

[10] L. B. Oliveira, D. F. Aranha, C. P. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Comput. Commun.*, vol. 34, no. 3, pp. 485–493, 2011.

[11] A. Capossele, C. Petrioli, G. Saturni, D. Spaccini, and D. Venturi, "Securing underwater communications: Key agreement based on fully hashed MQV," in *Proc. Int. Conf. Underwater Netw. & Syst. (WUWNet)*, 2017, pp. 1–5.

[12] M. Perillo, Z. Cheng, and W. Heinzelman, "An analysis of strategies for mitigating the sensor network hot spot problem," in *Proc. Int. Conf. Mobile Ubiq. Syst.: Netw. Serv.*, 2005, pp. 474–478.

[13] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 1, pp. 729–752, 2019.

[14] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in wireless sensor network: A survey," in *Proc. IEEE Int. Conf. Comput. Intel. and Comput. Research*, 2012, pp. 1–3.

[15] K. Bicakci, C. Gamage, B. Crispo, and A. S. Tanenbaum, "One-time sensors: A novel concept to mitigate node-capture attacks," in *European Workshop on Sec. in Ad-hoc Sens. Netw.* Springer, 2005, pp. 80–90.

[16] P. Tague and R. Poovendran, "Modeling adaptive node capture attacks in multi-hop wireless networks," *Ad Hoc Netw.*, vol. 5, no. 6, pp. 801–814, 2007.

[17] R. Garg, A. L. Varna, and M. Wu, "An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks," *IEEE Trans. Infor. Foren. Sec.*, vol. 7, no. 2, pp. 717–730, 2012.

[18] C. Lin and G. Wu, "Enhancing the attacking efficiency of the node capture attack in wsn: a matrix approach," *J. Supercomput.*, vol. 66, no. 2, pp. 989–1007, 2013.

[19] S. Agrawal, M. L. Das, and J. Lopez, "Detection of node capture attack in wireless sensor networks," *IEEE Systems J.*, vol. 13, no. 1, pp. 238–247, 2019.

[20] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. Comput. Commun. Sec.*, 2002, pp. 41–47.

[21] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security framework for underwater acoustic sensor networks," in *Proc. OCEANS – Genova*, 2015, pp. 1–9.

[22] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, 2016.

[23] M. A. Hamid, M. Abdullah-Al-Wadud, M. M. Hassan, A. Almogren, A. Alamri, A. R. M. Kamal, and M. Mamun-Or-Rashid, "A key distribution scheme for secure communication in acoustic sensor networks," *Future Gener. Comput. Syst.*, vol. 86, pp. 1209–1217, 2018.

[24] S. Zhang, X. Du, and X. Liu, "A secure remote mutual authentication scheme based on chaotic map for underwater acoustic networks," *IEEE Access*, vol. 8, pp. 48 285–48 298, 2020.

[25] H. Ma, J. Teng, T. Hu, P. Shi, and S. Wang, "Co-communication protocol of underwater sensor networks with quantum and acoustic communication capabilities," *Wirel. Pers. Commun.*, pp. 1–11, 2020.

[26] H. U. Yildiz, B. Tavli, B. O. Kahjogh, and E. Dogdu, "The impact of incapacitation of multiple critical sensor nodes on wireless sensor network lifetime," *IEEE Wirel. Commun. Let.*, vol. 6, no. 3, pp. 306–309, 2017.

[27] H. U. Yildiz, B. S. Ciftler, B. Tavli, K. Bicakci, and D. Incebacak, "The impact of incomplete secure connectivity on the lifetime of wireless sensor networks," *IEEE Systems J.*, vol. 12, no. 1, pp. 1042–1046, 2018.

[28] M. A. Khan, N. Javaid, A. Majid, M. Imran, and M. Alnuem, "Dual sink efficient balanced energy technique for underwater acoustic sensor networks," in *Proc. Int. Conf. Adv. Inform. Netw. Appl. Workshops (WAINA)*, 2016, pp. 551–556.

[29] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 11, no. 4, pp. 34–43, 2006.

[30] A. Ozmen, H. U. Yildiz, and B. Tavli, "Impact of minimizing the eavesdropping risks on lifetime of underwater acoustic sensor networks," in *Proc. Telecommun. Forum (TELFOR)*, 2020, pp. 1–4.